
Securing America's Cyber Future
A Mission-Critical Response to Evolving Threats
STRATIVIA®

Securing America's Cyber Future: A Mission-Critical Response to Evolving Threats

Introduction

Strativia understands that in today's hyperconnected federal landscape, Strativia understands that in today's hyperconnected federal landscape, **cybersecurity is not just a compliance checkbox—it's a mission enabler**. As agencies modernize systems and expand digital services, they become increasingly attractive targets for nation-state actors, cybercriminals, and insider threats.

Our federal clients—from the Department of Energy to the Department of Defense—look to us not only to support compliance, but to deliver **proactive, operationally relevant cybersecurity solutions**.

We approach cybersecurity as a **foundational component of mission assurance**. Whether supporting cleared intelligence operations in the Pacific or standing up NIST-compliant frameworks for civilian agencies, Strativia helps government leaders **anticipate risk, secure infrastructure, and execute with confidence**.

Understanding Today's Threat Environment

Strativia supports clients across diverse domains—from **classified energy programs** to **real-time logistics for TSA**—so we see firsthand how federal missions are being targeted by increasingly sophisticated cyber campaigns.

Ransomware, phishing, and supply chain infiltration are just the beginning. Adversaries are now leveraging **AI, deepfakes, and insider channels** to bypass traditional defenses.

Our cybersecurity support is built to address these threats **operationally**. Through **continuous monitoring**, **role-based access enforcement**, and **Zero Trust architecture design**, we enable our clients to stay mission-focused without compromising security posture.

Compliance is Table Stakes—Mission Assurance is the Goal

Strativia's cyber engagements go beyond simply meeting compliance requirements. We help our clients **operationalize federal frameworks**, including:

- **NIST SP 800-53 and 800-171**
- **RMF (Risk Management Framework)** for ATO readiness
- **CMMC** pre-assessment and implementation
- **FISMA and FedRAMP** policy compliance

In addition, we support development and maintenance of:

- Robust **Plan of Action and Milestones (POA&M)** systems
- Executive-level **stakeholder reporting dashboards**
- Mission-aligned **compliance summaries**—not just audit artifacts

Strativia's Cybersecurity Delivery Model

Our cybersecurity model is integrated across all phases of delivery—from **technical solutioning to executive governance**. Our **cleared professionals** operate both CONUS and OCONUS, supporting agencies like the Navy, TSA, and Department of Energy with:

- ISSO/ISSM support and continuous monitoring
- Configuration management and STIG enforcement
- Incident response and IOC operations
- Security engineering and ATO advisory services
- Identity and access management aligned to **Zero Trust principles**

We work side-by-side with agency stakeholders to **understand the mission, identify likely threats, and deploy the right people and tools** to defend against them.

Case Highlights: Strativia in Action

- **NNSA Cybersecurity Support**
  Full-scope information assurance and ATO support in classified environments.
- **TSA Information Assurance**
  IA delivery, vulnerability management, and RMF-compliant documentation across multiple task orders.
- **DOE & NIST**
  Zero Trust policy execution and FedRAMP advisory services aligned with CISA and OMB directives.
- **OCONUS Operations**
  Deployment of cleared cybersecurity professionals across **Bahrain and Japan** for mission continuity and defense IT support.

These engagements demonstrate Strativia's ability to **scale and adapt security operations** in dynamic environments—while maintaining full compliance and visibility.

The Strativia Commitment: Cybersecurity that Supports the Mission

Strativia combines the **rigor of a prime contractor** with the **responsiveness of a small business**. Our **ISO 27001-certified**, **CMMI Level 3–matured** security operations are purpose-built to help federal clients:

- Secure infrastructure
- Protect mission-critical data
- Preserve trust with the American public

When agencies partner with Strativia, they gain more than cybersecurity—they gain a **strategic delivery partner** who understands the mission, **accelerates compliance**, and builds **lasting resilience**.

Let's secure the mission—together.

Strativia (HQ)
1401 Mercantile Lane, Suite 501, Largo, MD 20774
P: 301-362-6555 | F: 301-362-6557
www.strativia.com

Strativia Regional Offices:
Arlington, VA | Atlanta, GA | Denver, CO